

## CLAIMS

1        1. A state-varying hybrid stream cipher operating within a computing device,  
2 comprising:  
3            a first software routine to divide incoming plain text into variable-sized blocks; and  
4            a second software routine to convert the plain text into cipher text based on an encryption  
5 key, an internal identifier and an internal state of the computing device.

1        2. The state-varying hybrid stream cipher of claim 1, wherein the first software  
2 routine produces the variable-sized blocks based on the encryption key, the internal identifier and  
3 an output of a first non-linear function.

1        3. The state-varying hybrid cipher of claim 2, wherein each current block of the  
2 plain text is determined by (i) producing a pseudo-random sequence using a second non-linear  
3 function including the encryption key, the internal identifier and the output of the first non-linear  
4 function as inputs and (ii) accessing contents of the pseudo-random sequence as a number of data  
5 elements of the plain text forming the current block.

1        4. The state-varying hybrid cipher of claim 1 further comprising:  
2            a third software routine to determine if a plurality of random data elements are to be  
3 distributed within the cipher text and to compute a hash digest of the random data elements.

4        5. The state-varying hybrid cipher of claim 4 further comprising a fourth software  
5 routine to perform a first shuffling operation on the internal state of the computing device based  
6 on the encryption key so that a single bit modification of the encryption key requires complete  
7 recalculation of the internal state of the computing device used to encrypt the random data  
8 elements.

1        6. The state-varying hybrid cipher of claim 4, wherein the second software routine  
2 further performs a second shuffling operation on the internal state of the computing device prior  
3 to encrypting the random data elements based on the encryption key and the internal identifier to

4 mitigate a likelihood of prediction of the internal state of the computing device upon knowledge  
5 of the encryption key.

1       7. The state-varying hybrid cipher of claim 4, wherein the third software routine  
2 determines a statistical amount of random data elements distributed within the cipher text is  
3 programmable based on a percentage value entered by a user.

1       8. The state varying hybrid cipher of claim 7, wherein the distribution of random  
2 data elements within the cipher text is based on the encryption key, the internal identifier and  
3 internal state of the computing device.

1       9. The state-varying hybrid cipher of claim 1 further comprising a third software  
2 routine to distribute error correcting codes in the cipher text in order to correct modifications.

1       10. The state-varying hybrid cipher of claim 1, wherein the internal state of the  
2 computing device is periodically modified.

1       11. The state-varying hybrid cipher of claim 1, wherein the internal state of the  
2 computing device is based on a time value.

1       12. A computing device comprising:  
2           a memory; and  
3           logic to perform a state-varying stream cipher operation, controlled by at least an  
4           encryption key and an internal state of the computing device, on input data segmented in random  
5           sized blocks.

1       13. The computing device of claim 12, wherein the stream cipher operation involves  
2           encryption.

- 1        14. The computing device of claim 12, wherein the logic is an integrated circuit.
- 1        15. The computing device of claim 12, wherein the internal state of the computing  
2 device varies over time.
- 1        16. The computing device of claim 15, wherein the variation of the internal state of  
2 the computing device is periodic being set at a time that an encryption process begins for each  
3 block of input data.
- 1        17. The computing device of claim 12, wherein the computing device is a smart card.
- 1        18. The computing device of claim 15, wherein the logic of the computing device is  
2 an operating system.
- 1        19. A method for decrypting input data using a combination of stream cipher and  
2 block cipher functionality, comprising:  
3            receiving as input a cipher text, a decryption key, a percentage of random data and a  
4 unique internal identifier; and  
5            reiteratively decrypting blocks of the cipher text using the decryption key, the  
6 percentage of random data, the unique internal identifier and a varying internal state of the  
7 computing device to recover corresponding blocks of plain text.
- 1        20. The method of claim 19, wherein the internal state of the computing device varies  
2 over continuously over time.